



BLOCKCHAIN TECNOLOGIA

JOÃO VITOR MONTANARI DA SILVA

SUMÁRIO

O QUE É BLOCKCHAIN



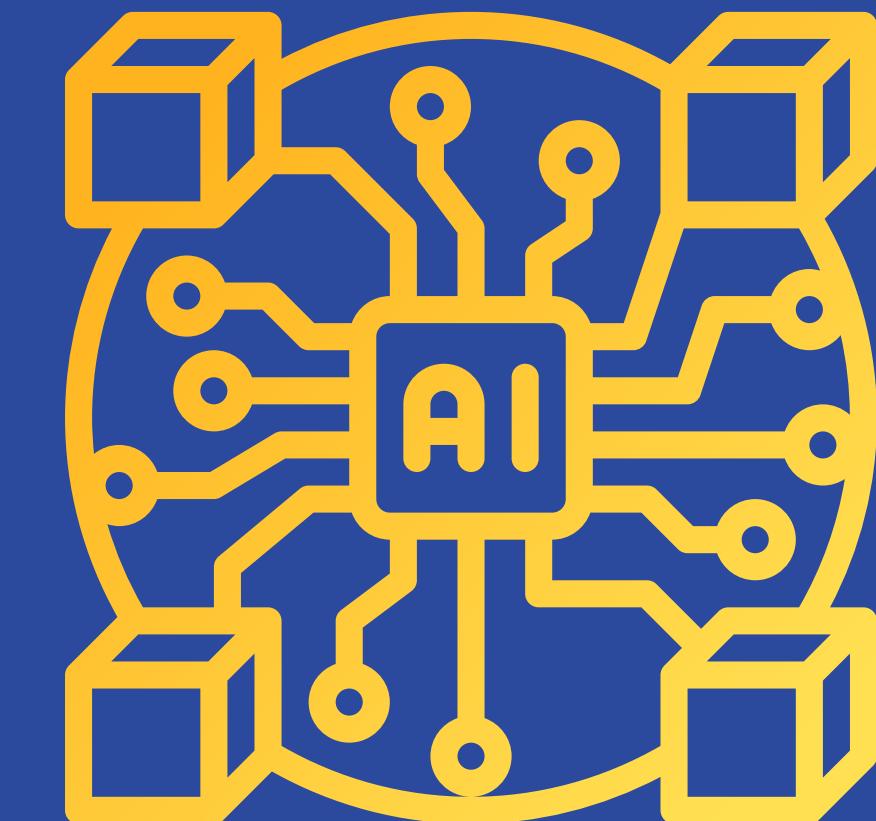
PRINCIPAIS ELEMENTOS

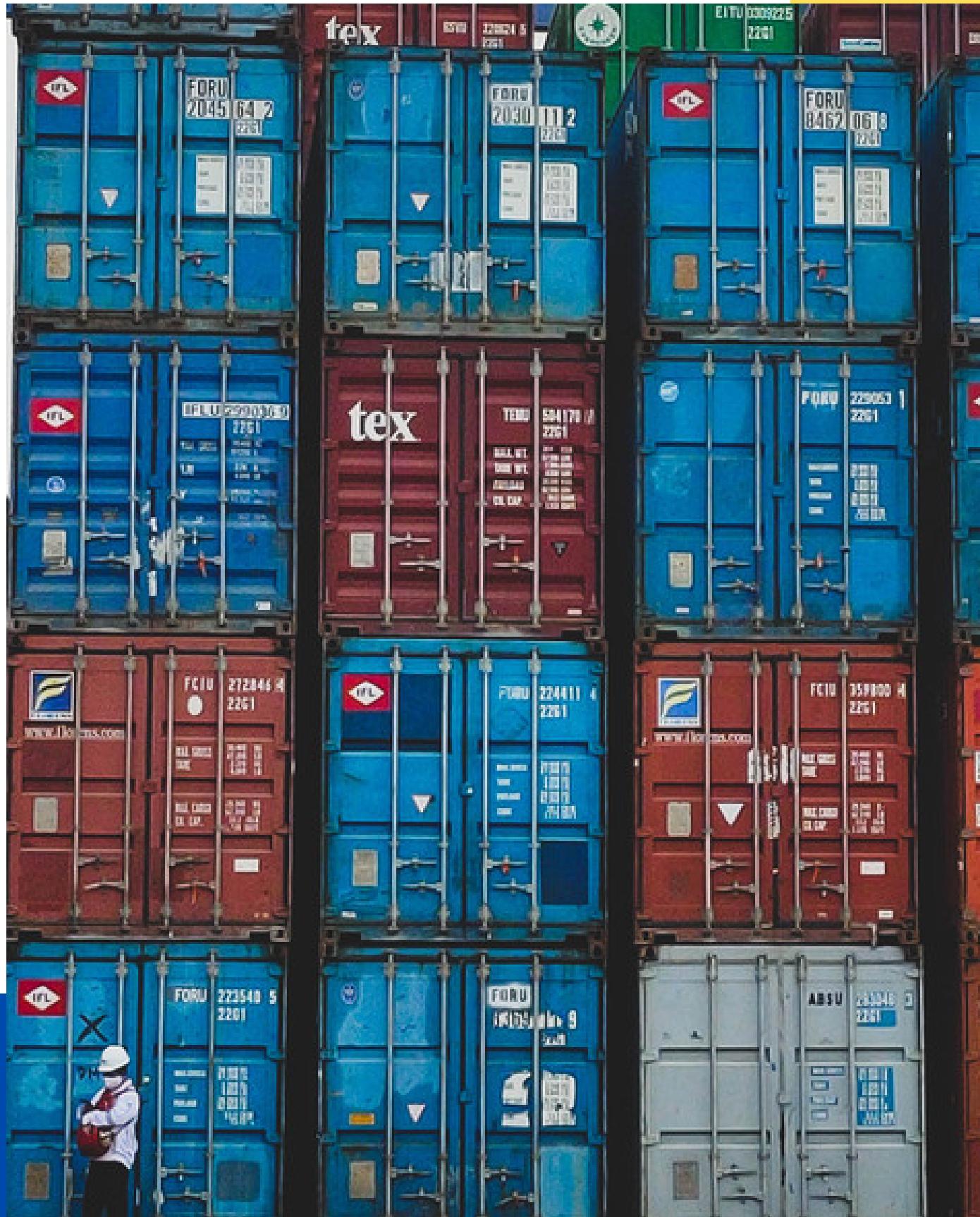


TIPOS DE REDE BLOCKCHAIN



COMO CONSTRUIR UMA BLOCKCHAIN





O QUE É A TECNOLOGIA DE BLOCKCHAIN



Blockchain é uma tecnologia de registro distribuído que permite a criação de um registro compartilhado, seguro e permanente de transações. Ela foi originalmente criada como base para a criptomoeda Bitcoin, mas desde então tem sido amplamente aplicada em uma variedade de outros usos, incluindo contratos inteligentes, votações eletrônicas e registros de propriedade.

O QUE É A TECNOLOGIA DE BLOCKCHAIN

Em um blockchain, cada transação é adicionada a um "bloco" e cada bloco é conectado aos blocos anteriores em uma cadeia contínua, daí o nome "blockchain". Isso torna difícil para qualquer pessoa alterar ou apagar transações passadas, pois isso exigiria alterações em todos os blocos subsequentes da cadeia. Além disso, os dados são replicados em todas as cópias da rede, tornando-os acessíveis e seguros contra falhas de hardware.



Blockchain oferece um novo modelo de confiança baseado em consenso e matemática, ao invés de terceiros confiáveis, como bancos ou governos. Isso permite que partes sem confiança entre si possam colaborar e transacionar de forma segura sem a necessidade de intermediários.

PRINCIPAIS ELEMENTOS DE UMA BLOCKCHAIN

oooo

oooo



PRINCIPAIS ELEMENTOS DE UMA BLOCKCHAIN



Tecnologia de livro-razão

O "Ledger" (Livro-Razão, em português) é a estrutura básica da blockchain que registra e armazena todas as transações e informações relevantes da rede. É uma lista encadeada de blocos, onde cada bloco contém informações sobre transações ou dados adicionais. Cada novo bloco é ligado ao bloco anterior, tornando a blockchain uma estrutura de dados imutável e confiável. O Ledger é mantido e atualizado por todos os nós da rede, garantindo que a informação seja distribuída de forma descentralizada e segura.

PRINCIPAIS ELEMENTOS DE UMA BLOCKCHAIN

Registros imutáveis

Registros imutáveis na blockchain são informações registradas na blockchain que não podem ser alteradas ou apagadas após serem adicionadas à cadeia. Isso é conseguido através da utilização de algoritmos de criptografia forte que garantem a integridade dos dados.

A imutabilidade dos registros na blockchain é uma das suas principais características, permitindo que ela seja usada como uma forma confiável de registrar informações em aplicações. Além disso, a imutabilidade dos registros na blockchain contribui para a transparência e confiança nas transações registradas na cadeia, já que todos os nós da rede têm acesso às informações e podem verificar sua integridade.



PRINCIPAIS ELEMENTOS DE UMA BLOCKCHAIN



Contratos inteligentes

Contratos inteligentes na blockchain são programas de computador que são armazenados e executados na blockchain. Esses contratos podem ser usados para definir regras e condições para transações e interações na blockchain, automatizando processos e tornando-os mais seguros e confiáveis.

Os contratos inteligentes são programados com base em condições específicas e só são executados quando essas condições são atendidas. Eles funcionam como um acordo automatizado entre duas ou mais partes, garantindo que as transações sejam realizadas de acordo com as regras pré-estabelecidas.



Imutabilidade:

As informações armazenadas na blockchain são permanentes e não podem ser alteradas ou apagadas, o que as torna confiáveis.



Automatização:

A utilização de contratos inteligentes na blockchain permite a automatização de processos, tornando-os mais eficientes e confiáveis.



Eficiência:

As transações realizadas na blockchain são geralmente mais rápidas e mais eficientes do que as realizadas por meio de intermediários tradicionais.



Baixos custos:

A eliminação de intermediários nas transações pode levar a uma redução dos custos envolvidos.

BENEFÍCIOS DA BLOCKCHAIN



Segurança:

A blockchain é projetada para ser imutável, o que significa que as informações armazenadas nele são extremamente seguras e difíceis de serem alteradas ou hackeadas.



Transparência:

A blockchain permite a transparência das transações, o que significa que todas as partes envolvidas em uma transação têm acesso aos detalhes da mesma.



Descentralização:

A blockchain não é controlada por uma única entidade, o que significa que as informações e transações são mantidas por uma rede distribuída de usuários.

Tipos de rede de blockchain

Existem várias formas de criar uma rede de blockchain. Essas redes podem ser:

- Públicas;
- Privadas;
- Permissionárias;
- Consórcio.



REDES DE BLOCKCHAIN PÚBLICAS

Redes de blockchain públicas são sistemas de registro distribuídos que podem ser usados por qualquer pessoa sem restrições ou permissões. Nelas, qualquer usuário pode participar da validação de transações, realizar transações, criar e gerenciar contratos inteligentes e validar novos blocos na cadeia. A segurança da rede é garantida por uma combinação de criptografia, consenso e incentivo econômico. Exemplos de redes de blockchain públicas incluem Bitcoin, Ethereum e Litecoin.



REDES DE BLOCKCHAIN PRIVADAS

Redes de blockchain privadas são sistemas de registro distribuídos que são restritos a um grupo selecionado de participantes. Em contraste com as redes públicas, onde qualquer pessoa pode participar, as redes privadas geralmente são usadas por empresas, organizações governamentais ou consórcios para fins específicos. Em uma rede privada, a validação de transações é realizada por um grupo selecionado de nós autorizados, e as transações só podem ser realizadas por participantes autorizados.

A segurança é garantida por meios semelhantes aos de uma rede pública, como criptografia, consenso e incentivos econômicos, mas é geralmente reforçada pela restrição a um grupo menor de participantes. Exemplos de redes privadas incluem a rede Enterprise Ethereum Alliance e a plataforma Hyperledger Fabric.



REDES DE BLOCKCHAIN PERMISSIONÁRIAS

Redes de blockchain permissionárias são um tipo de rede blockchain privada, em que os participantes precisam ter permissão para participar da rede e realizar transações. Em uma rede permissionária, existe um administrador ou grupo de administradores responsável por conceder permissões de acesso aos participantes e regulamentar o uso da rede.

A validação de transações é realizada por um subconjunto de nós autorizados, garantindo que a rede seja mais rápida e escalável do que as redes públicas. Além disso, a segurança é geralmente reforçada pela restrição a um grupo menor de participantes.

No entanto, o fato de que somente participantes autorizados podem participar e realizar transações significa que a descentralização é limitada. Exemplos de redes permissionárias incluem a rede R3 Corda e a plataforma Hyperledger Sawtooth.

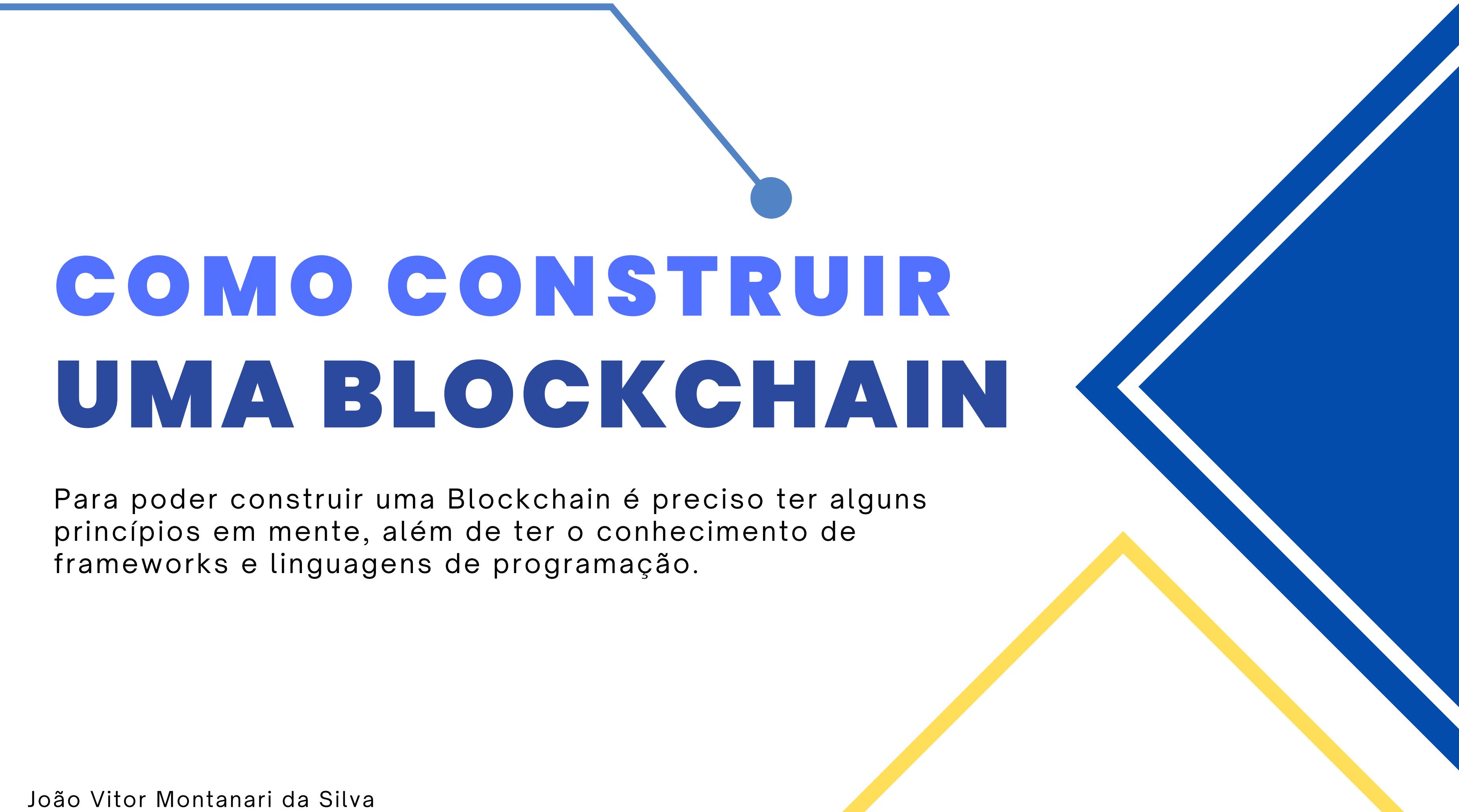


BLOCKCHAINS DE CONSÓRCIO

Blockchains de consórcio são uma forma de tecnologia blockchain projetada para uso em grupos específicos de participantes, como empresas de uma mesma indústria.

Em vez de serem totalmente públicos ou totalmente privados, as blockchains de consórcio permitem que apenas membros autorizados participem da rede e validem transações. Isso permite aos membros do consórcio trabalhar juntos em uma base de confiança sem a necessidade de uma autoridade central ou intermediários.





COMO CONSTRUIR UMA BLOCKCHAIN

Para poder construir uma Blockchain é preciso ter alguns princípios em mente, além de ter o conhecimento de frameworks e linguagens de programação.

PROGRAMAR BLOCKCHAIN:



Para programar uma blockchain, é preciso ter conhecimento em programação, conhecer a arquitetura de blockchain e entender como funcionam os conceitos de consensus, criptografia, hash e ledgers distribuídos.

Além disso, é importante escolher uma linguagem de programação adequada, como Python, JavaScript, C ++ ou Go. A implementação da blockchain pode ser feita passo a passo, começando pelo design de uma estrutura de dados para armazenar as transações e os blocos, seguido da implementação do algoritmo de consenso para confirmação das transações.

Depois disso, é preciso implementar as regras de negócio, a API para acessar a blockchain e as funcionalidades para adicionar e validar novos blocos e transações. Finalmente, testar e otimizar o sistema é crucial para garantir a segurança, a escalabilidade e a confiabilidade da blockchain.

PRINCIPIOS PARA A CONSTRUÇÃO:

1

Defina o objetivo da sua blockchain: O que você quer alcançar com sua blockchain? É uma aplicação financeira, uma plataforma de votação, um sistema de gerenciamento de ativos, etc.

2

Escolha uma arquitetura de consenso: A arquitetura de consenso é a forma como a rede consensua sobre a validade das transações e dos blocos. Algumas opções incluem Proof of Work, Proof of Stake e Delegated Proof of Stake.

3

Desenvolva o seu protocolo: Escreva o código que define como as transações serão validadas e adicionadas aos blocos.

4

Implemente a camada de rede: Crie a estrutura da sua rede, incluindo as regras para a adição de nós, a transmissão de mensagens entre nós, etc.

5

Teste e valide sua blockchain: Teste intensivamente sua blockchain para garantir que esteja funcionando corretamente antes de colocá-la em produção.





PLATAFORMAS PARA BLOCKCHAIN:

0 0 0 0

Ethereum:

Ethereum é um framework de blockchain descentralizado que permite a criação e execução de contratos inteligentes e aplicações descentralizadas. Ele foi lançado em 2015 e é baseado na tecnologia blockchain, permitindo aos desenvolvedores criar e executar aplicativos descentralizados sem a necessidade de terceiros.

O Ethereum é programado principalmente em linguagem de programação Solidity e utiliza sua própria criptomoeda, o Ether, para financiar transações e incentivar os nós da rede a executar contratos inteligentes.

Além disso, o Ethereum oferece uma ampla gama de ferramentas e recursos para desenvolvedores, incluindo a plataforma de desenvolvimento Ethereum, bibliotecas e ferramentas de gerenciamento de contratos inteligentes.



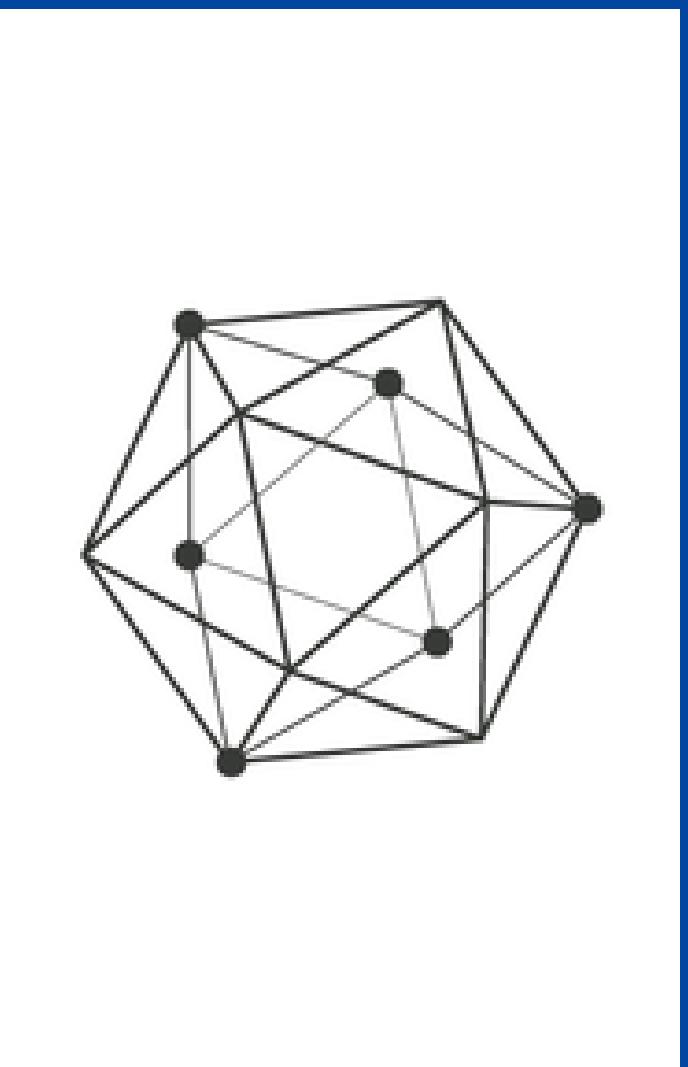
PLATAFORMAS PARA BLOCKCHAIN:

Hyperledger:

Hyperledger é um projeto de código aberto patrocinado pelo Linux Foundation, que tem como objetivo fornecer soluções de blockchain empresarial. O Hyperledger inclui uma série de frameworks e ferramentas que ajudam as empresas a desenvolver, implantar e gerenciar aplicativos de blockchain.

Alguns dos frameworks incluídos são o Hyperledger Fabric, Hyperledger Sawtooth, Hyperledger Indy e Hyperledger Iroha. O Hyperledger Fabric é o mais amplamente utilizado para aplicativos empresariais, pois oferece alta escalabilidade e segurança.

Além disso, o Hyperledger fornece ferramentas de gerenciamento de identidade, contratos inteligentes e integração de aplicativos, tornando mais fácil para as empresas implementar soluções de blockchain.



PLATAFORMAS PARA BLOCKCHAIN:

Multichain:

Multichain é um framework de código aberto para construir blockchains personalizados. Ele oferece uma série de recursos para gerenciar e controlar a rede de blockchain, incluindo privilégios de administrador, criação de ativos, identidades e autorizações.

Além disso, ele permite a integração de aplicativos externos e a customização de regras de consenso para atender às necessidades específicas de cada rede de blockchain.

Com sua arquitetura flexível e escalável, o Multichain é uma boa escolha para empresas e organizações que procuram criar soluções blockchain personalizadas.



PLATAFORMAS PARA BLOCKCHAIN:

Chaincode:

Chaincode é uma linguagem de programação usada para escrever aplicações descentralizadas (smart contracts) na plataforma Hyperledger Fabric. É executado como parte de um nó de rede na blockchain e é responsável por gerenciar as transações e atualizações de estado na blockchain.

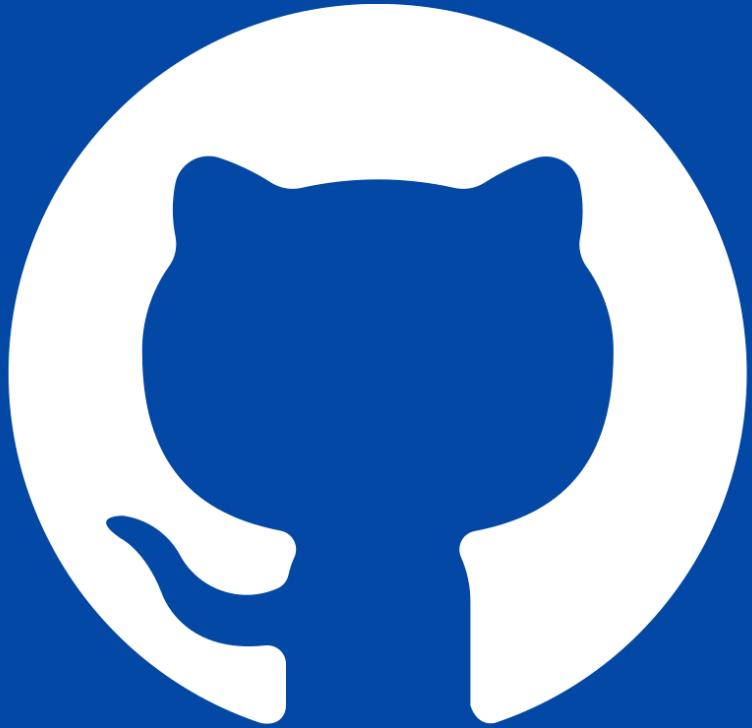
Com o Chaincode, os desenvolvedores podem implementar funcionalidades customizadas, como a gestão de ativos digitais, contratos financeiros e votações na rede.

O Chaincode também oferece segurança e privacidade, garantindo que somente os membros autorizados da rede possam acessar e modificar as informações.



oooo

Espero que tenha gostado!



joao-montanari



João V. Montanari



oooo